

Term	Action	Description/Notes	Current Definition		Source
AM	Add	Acronym		After Action Meeting	FEMA
AAR	Add	Acronym		After Action Report	FEMA
				The AAM is a meeting held among elected and appointed officials or their designees	
				from the exercising organizations, as well as the lead evaluator and members of the	
				exercise planning team, to debrief the exercise and to review and refine the draft	
				AAR/IP. The AAM should be an interactive session, providing attendees the	
				opportunity to discuss and validate the analytical findings and corrective actions in	
After Action Meeting (AAM)	Add			the draft AAR/IP.	FEMA
After Action Report (AAR)	Add			A document containing findings and recommendations from an exercise or a test.	NIST
			From an information technology perspective, in the agency's opinion, the loss of this	See , Application Criticality.	
		Renamed term from "Department	application will have a direct impact to this department's core functions, processes		
Agency Critical	Modify	Critical" and modified definition	and/or activities.		FEMA
			The spectrum of all types of hazards including accidents; technological events; natural	A classification encompassing all conditions, environmental or human-caused, that	
			disasters; terrorist attacks; warfare; and, chemical, biological (including pandemic	have the potential to cause injury, illness, or death; damage to or loss of equipment,	
			influenza), radiological, nuclear, or explosive events.	infrastructure services, or property; or alternatively causing functional degradation	
			, , , , , , , , , , , , , , , , , , ,	to social, economic, or environmental aspects. These include accidents, technological	
				events, natural disasters, space weather, domestic and foreign-sponsored terrorist	
				attacks, acts of war, weapons of mass destruction, and chemical, biological (including	
				pandemic), radiological, nuclear, or explosive events.	
II_Hazards	Modify				FEMA
ll-Hazards	Modify		Alternate sites are legations of borthon the universe facility and the same of		FEIVIA
	1		Alternate sites are locations other than the primary facility used to carry out Essential	Fixed, mobile, or transportable locations, other than the primary operating facility,	
	1	Danamada va Garaga	Functions by relocating ERG members following activation of the Continuity Plan.	where leadership and continuity personnel relocate in order to perform essential	
	1.	Renamed term from "Alternate		functions following activation of the continuity plan.	
Iternate Locations	Modify	Sites" and modified definition	and mobile work concepts.		FEMA
			A computer system (potentially including multiple programs, modules, etc.) designed	A software program hosted by an information system. This is in contrast to software	
				such as operating systems.	
			Applications typically fall into one of four categories: Core Business; Desktop; Common		
			Services & Integration; and Process Automation. It is also a generic term for a program		
pplication	Modify		or system that handles a specific business function.		NIST
			Application Criticality – Application criticality has the following categories.	Application Criticality – Application criticality has the following categories.	
			• Statewide Critical – From an information technology perspective, in the agency's	• Statewide Critical – Based on the agency's analysis, this application has a direct	
			opinion, the loss of this application will have a direct impact to statewide core	impact to statewide essential functions, processes, activities, or population.	
1			functions, processes and/or activities. The applications loss may also impact a large		
			portion of the State's population.	Agency Critical – Based on the agency's analysis, this application has a direct	
				impact to this agency's essential functions, processes and/or activities.	
			• Department Critical – From an information technology perspective, in the agency's		
			opinion, the loss of this application will have a direct impact to this department's core	Program Critical – Based on the agency's analysis, this application has a direct	
			functions, processes and/or activities.	impact to the essential functions, processes and/or activities associated with a	
			Turictions, processes and/or activities.		
			Program Critical From an information tachnology parameting in the agency's	program within the agency.	
			Program Critical – From an information technology perspective, in the agency's animies, the loss of this application will have a direct impact to the gare functions.	A Non Critical Posed on the agency's analysis this any limiting house directions	
			opinion, the loss of this application will have a direct impact to the core functions,	• Non-Critical – Based on the agency's analysis, this application has no direct impact	
			processes and/or activities associated with a program within an agency.	to a state, agency, or program's essential functions, processes and activities within	
	1			the agency.	
	1		• Non Critical – From an information technology perspective, in the agency's opinion,		
	1		the loss of this application will have little or no impact to statewide and/or this		
	1		department's core functions, processes and activities or the core functions, processes		
pplication Criticality	Modify		and activities associated with a program within an agency.		FEMA
				Anything that has value to an organization, including, but not limited to, another	
				organization, person, computing device, information technology (IT) system, IT	
				network, IT circuit, software (both an installed instance and a physical instance),	
				virtual computing platform (common in cloud and virtualized computing), and	
sset	Add			related hardware (e.g., locks, cabinets, keyboards).	NIST
PA	Add	Acronym		Business Process Analysis	FEMA
5,77		,	A management level analysis, which identifies the impacts of losing organizational	A method of identifying the consequences of failing to perform a function or	
			information technology resources. A BIA measures the effect of resource loss and	requirement.	
			escalating losses over time, in order to provide senior management with reliable data	. 545 5 5	
usiness Impact Analysis (BIA)	Modify				FEMA
daniesa impact Alialysis (DIA)	Iviouity		upon which to base decisions on risk mitigation and continuity planning.	A mothod of examining identifying and manning the functional assesses	LIVIA
			A method of examining, identifying, and mapping the functional processes, workflows,		
	 		activities, personnel expertise, systems, data, interdependencies, and facilities	workflows, activities, personnel expertise, systems, data, interdependencies, and	FF. 4 :
Business Process Analysis (BPA)	Modify		inherent in the execution of a function or requirement.	alternate locations inherent in the execution of a function or requirement.	FEMA



Continuity Coordinator Continuity Coordinator Continuity Coordinator Continuity Coordinator Continuity Coordinator Add Continuity Coordinator Continuity Coordinator Continuity Coordinator Continuity Coordinator Continuity Coordinator Coordinator Continuity Coordinator	present at the d to activate the re and intilation and air linitaining srupts normal linctions, using een integrated ring of our form of nance of NEFs and linitaining of our form of nance of serious are linitations.	FEMA NIST FEMA
A facility that is retire tradition on operational on a daily basis. Electromication, 12 equations to a daily basis. Electromication, 12 equations are specialized personnel must be deployed by facilities. Add Add Add Add Add Add Add Add	resent at the d to activate the re and ntilation and air intaining srupts normal inctions, using een integrated ring of our form of nance of NEFs and officials, who is redinators are	FEMA NIST FEMA
Telecommunications, IT equipment, und inhabituature is typically in batton, however trans of specialized personnel must be exployed years before the site can become operational. Seas infrastructure environmental controls on Specialized personnel must be exployed years before the site can become operational. Seas infrastructure environmental controls on Specialized personnel must be exployed years before the site can become operational. Seas infrastructure environmental controls on specialized personnel must be exployed years before the site can become operational. Seas infrastructure environmental controls on specialized personnel seas of control of the properties of the season o	d to activate the re and ntilation and air limitaining srupts normal limitaining een integrated ring of our form of nance of NEFs and officials, who is redinators are	NIST FEMA
ocation, however teams of specialized genome must be deployed systems before the sist on a become operational, absorbing many continuously active. Add An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. Continuity Modify And An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. Continuity Add An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. COOP and COO ground after an indicent that of the continuity of provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an event. COOP and COO ground and after an indicent that of the continuity perform its specified in the continuity of the continuity program. Continuity of the continuity program. Continuity of the continuity program. Continuity of the continuity program continuity program. Continuity of severement to continuity program. Continuity of severement to continuity program. Continuity of severement to continuity of severement to continuity of severement. Continuity of Government (COO) Modify Term was removed The presentation, maintenance, or reconstitution of oil government's ability to continuity of elected officials at all levels of government to continuity of elected officials at all levels of government to the continuity program. Continuity of elected officials at all levels of government to continuity of elected officials at all levels of government to continuity of elected officials at all levels of government to continuity of elected officials at all levels of government to continuity of elected officials at all levels of government to continuity of elected officials at all levels of government to continuity of elected offic	d to activate the re and ntilation and air limitaining srupts normal limitaining een integrated ring of our form of nance of NEFs and officials, who is redinators are	NIST FEMA
ocation, however teams of specialized genome must be deployed systems before the site of an become operational, absorbing management out to deployed systems before the site of an become operational, absorbing management of the straing ventor controlling systems, yet gottom or management of the straing ventor and of the straing v	d to activate the re and ntilation and air limitaining srupts normal limitaining een integrated ring of our form of nance of NEFs and officials, who is redinators are	NIST FEMA
oditise Add Add Add Add Add Add Add A	ntilation and air intilation and air intaining srupts normal inctions, using een integrated ring of our form of nance of NEFs and officials, who is rdinators are	NIST FEMA
continuity Capability Add Add An uninterrupted ability to provide services and support, while maintaining organizational visibility, before, during, and after an event. Add An uninterrupted ability to provide services and support, while maintaining organizational visibility, before, during, and after an event. Add An uninterrupted ability to provide services and support, while maintaining organizational visibility, before, during, and after an event. COOP and COG programs and continuity requirements that have be into the organization of continue to perform its assential in. COOP and COG programs and continuity requirements that have be into the organizational visibility. Defore, during, and after an event. Add The selling of an organization or continue to perform its assential in. COOP and COG programs and continuity requirements that have be into the organizational coveragin of the continuity program. Continuity or an organizational exempts of the U.S. Constitution and the continued perform organizational exempts of the U.S. Constitution and the continued perform organizational exempts of the continued perform organizational exempts of the continued perform organizational exempts of the U.S. Constitution and the continued perform organizational exempts of the continued perform organizational exempts of the U.S. Constitution and the continued perform organizational exempts of the continued perform organizational exempts of the U.S. Constitution and the continued perform organizational exempts of the U.S. Constitution and the continued perform organizational exempts of the U.S. Constitution and the continued perform organization organizational exempts of the U.S. Constitution organization organiz	ntilation and air intaining srupts normal inctions, using een integrated ring of our form of nance of NEFs and officials, who is rdinators are	NIST FEMA
continuity Coordinator Add Add Add Add An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. The ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an event. Add Add Add Add Add Add Add A	intaining srupts normal inctions, using een integrated ring of our form of nance of NEFs and officials, who is rdinators are	NIST FEMA
Continuity Coordinator Add An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. Ontinuity Modify Add And Uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. The ability of an organizational viability of an organization continuity requirements that have being organizational viability of an organization of polyment and the continuity perform its essential functions. The primary goal is preserved organizational essential functions estimate the continuity perform organizational essential functions. The primary goal is preserved organizational essential functions estimated by the organization or government seves throughout the organization or government seves throughout the organization or government as agency management in the statewise information Security Management and Continuity Security of Continuity Parisons or an application of civil governments ability to curry of that essential functions continue to be performed before, during, a employed of any unnergency condition that could disrupt such processes and services. A coordinated effort within the executive, legislative and judical processes under the threat or occurrence of any unnergency condition that could disrupt such processes and services. A conditional (COCCON) Remove Immune Add Acronym The preservation, maintenance, or reconstitution of civil governments and applications or continuity of Government for whithin the executive, legislative and judical processes under the threat or occurrence of any unnergency condition that could disrupt such processes and services. A conditional (COCCON) Remove Immune Add Acronym The preservation, maintenance, or reconstitution of civil governments and services. A ded Acronym The preserv	intaining srupts normal inctions, using een integrated ring of our form of nance of NEFs and officials, who is rdinators are	NIST FEMA
And uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. And uninterrupted ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an event. The ability of an organization to continue to perform its sesential in Operations. The polity of an organization shall provide uninterrupted services and support, while maintaining organization advability, before, during, and after an event. The ability of an organization to continue to perform its sesential in COOP and COO pergrams and continue year-gimentum that have be into the organization of primary goal is present government, despite the organization of continuely performed before exponsible for coveragit of the continuity performed before exponsible for overagition of the continuity performed before the organization of continuity performed before despite exponsible for overagition of the continuity performed before despite exponsible for overagition of the continuity performed before despite exponsible for overagition of the continuity performed before despite exponsible for overagition of the continuity performed before despite exponsible for overagition of the continuity performed before despite exponsible for overagition of the continuity performed before despite exponsible for overagition of the continuity performed before despite exponsible for overagition of the continuity performed before despite the performance of the continuity of coverament to the continuity of coverament to the performance of the continuity of coverament to the executive, legislative, or judicial breaching and the continuity of coverament to the executive, legislative and judicial processes under the threat or occurrence of the executive performed before, during a many emergency condition that could disrupt such processes and services. The performance of the performance before the performance of the performance of the performance of the	intaining srupts normal inctions, using een integrated ring of our form of nance of NEFs and officials, who is rdinators are	FEMA
An uninterrupted ability to provide services and support, while maintaining organizational viability, but of continuity organizational viability, but of continuity organizational viability, but organizational viability, but organizational viability of provide uninterrupted services and support, while maintaining organizational viability of continuity requirements that have be into the organizational viability of personal to continue to perform as essential fructions and the continuity organization and preform organizations delign operations. Add Add Add Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Term was removed The maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Term was removed Add Acronym Term was removed Term was remo	intaining srupts normal inctions, using een integrated ring of our form of nance of NEFs and officials, who is rdinators are	FEMA
organizational viability, before, during, and after an event. organizational viability, before, during, and after an event. operations CDCP and CDG programs and continuity requirements that have be not be performed obtained to the organization of continuity of an organization of continuity organization of continuity organization of continuity organizations or poverment under the U.S. Constitution and the continuity program. Continuity organizations or poverment under the U.S. Constitutions and the continuity organization or government. Add The senior accountable official, dissignated by leadership or elected responsible for oversight of the continuity program. Continuity organization or government. As a gency management of the Statewish Information Security Man Continuity Facilities Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative, or judicial bra out the executive organization or government or any emergency condition that could disrupt such processes and services. Continuity of Government (COG) Modify Term was removed Term wa	en integrated ring of our form of nance of NEFs and officials, who is rdinators are	
Continuity Coordinator Continuity Coordinator Continuity Coordinator Continuity Coordinator Continuity Coordinator Continuity Government Loos Continuity Facilities Term was removed Term was rem	inctions, using een integrated ring of our form of nance of NEFs and officials, who is rdinators are	
The ability of an organization to continue to perform its essential for COOP and COG programs and continuity requirements that have be into the organizations' daily operations. The primary goal is preserve powerment under the U.S. Constitution and the continued perform organizational essential functions under all conditions. The senior accountable official, designated by leadership or elected responsible for oversight of the continuity program. Continuity coordinator Add The senior accountable official, designated by leadership or elected responsible for oversight of the continuity program. Continuity coordinator Add The senior accountable official, designated by leadership or elected responsible for oversight of the continuity program. Continuity coordinator Add The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative, and judicial processes under the threat or occurrence of amy emergency condition that could disrupt such processes and services. The senior accountable official is at all levels of government (COG) Modiffy Continuity of Government (COG) Modiffy The rem was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative, and judicial processes under the threat or occurrence of amy emergency condition that could disrupt such processes and services. The accountable of the preservation of the preservation of continuity of Government (COG) The senior accomment (COG) The senior accountable of the preservation of continuity of Government (COG) The preservation of the preservation of continuity of Government (COG) The senior accomment (COG) The senior accommen	een integrated ring of our form of nance of NEFs and officials, who is rdinators are	
COOP and COG programs and continuity requirements that have to into the organization of sopial is present government under the U.S. Constitution and the continued perform organizations assential functions under all conditions. Add The senior accountable official, designated by leadership or elected responsible for oversight of the continuity program. Continuity panager and other continuity panager and continuity panager and continuity panager and other continuity panager and other continuity panager and continuity panager and continuity panager and continuity panager and continuity panag	een integrated ring of our form of nance of NEFs and officials, who is rdinators are	
Into the organization's daily operations. The primary goal is present organization and second time of the U.S. Constitution and the continued perform organizational essential functions under all conditions. The senior accountable official, designated by leadership or elected responsible for oversight of the continuity pragmers or subported by a continuity of supported by a continuity palmers or subcomponent levels throughout the organization or government. Add Continuity Coordinator Add Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judical processes under the threat or occurrence of any emergency orthogory of the continuity of covernment (COG) Modify Modify Modify Modify Modify Modify Modify Add Acronym Add Acronym Computer Security incident Response Plan, See, Incident Response Plan, See, Incident Response Plan, See, Cyber Incident Response Team (CRT) Add Acronym Computer Security incident Response Plan, See, Cyber Incident Response Team (CRT) Add Acronym Computer Security incident Response Plan, See, Cyber Incident Response Team (CRT) Add Acronym Computer Security incident Response Plan, See, Cyber Incident Response Team (CRT) An Individual or a group posing a cyber threat. This threat can be divided within an organization by travel users of rom emented coations be persons using the Internet. Threats can come from numerous sour nostile governments is terrorist group, digrantide employers and instrument to full such as committing fraud, trafficking in child pornography and intellects. A cyber Threat Actor who uses a computer as an instrument to full such as committing fraud, trafficking in child pornography and intellects.	ring of our form of nance of NEFs and officials, who is rdinators are	
portinuity Capability Add The senior accountable official, designated by leadership or elected responsible for oversight of the continuity program. Continuity consisting of several responsible for oversight of the continuity program. Continuity consumers as a gancy management in the Statewide Information Security Man Continuity Facilities Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Modify Modify Add Acronym Computer Security incident Response Plan, Sec, Judicial Response Plan, Sec, Upter Incident Response Team Add Acronym Add Acronym Add Acronym Computer Security incident Response Plan, Sec, Cyber Incident Response Team Add Acronym Acronym Add Acronym	nance of NEFs and officials, who is rdinators are	
ontinuity Capability Add The senior accountable official, designated by leadership or elected responsible for oversight of the continuity program. Continuity conditions supported by a continuity manager and other continuity planners versus subcomponent levels throughout the organization or government. as agency management in the Statewiske information Security Man Continuity Facilities Remove Term was removed The preservation, maintenance, or reconstitution of tivil governments ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Ontinuity of Government (COG) Modity Ontinuity of Government (COG) Remove Term was removed Term was removed Ontinuity of Government (COG) Add Acronym Computer Security incident Response Plan, See, Incident Response Plan, See, Incident Response Plan, See, Cyber Incident Response Team Add Acronym Computer Security incident Response Plan, See, Cyber Incident Response Plan, See, Cyber Incident Response Team, Add Acronym Computer Security incident Response Plan, See, Cyber Incident Response Plan, See, Cyber Threat Actor Group of Individuals usually consisting of Security Analysts organize recommend, and coordinate immediate mitigation actions for conternations or a person using the Internet. Threats can come from numerous sour hostile governments, sterorist groups, disgrunted employees, and within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous sour hostile governments, sterorist groups, disgrunted employees, and intrudees. Add Action of the preservation of the pre	officials, who is rdinators are	
ontinuity Coordinator Add The semior accountable official, designated by leadership or elected responsible for oversight of the continuity planners we subcomponent levels throughout the organization or government, as agency management in the Statewide Information Security Man Continuity Facilities Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. any emergency condition that could disrupt such processes and services. and unitable of the executive, legislative, or judicial bracesses under the threat or occurrence of any emergency or threat. Continuity of government (COG) Modify ontinuity of Government eadiness Conditions (COGCON) Remove Term was removed SIRP Add Acronym Computer Security incident Response Plan, See, Incident Response Plan, See, Cyber Incident Response Team (IRT) Add Acronym Computer Security incident Response Team, See, Cyber Incident Re	officials, who is rdinators are	
The senior accountable official, designated by leadership or elected responsible for oversight of the continuity program. Continuity countinuity Coordinator Add Continuity Coordinator Add Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Term was removed Term w	officials, who is rdinators are	
responsible for oversight of the continuity program. Continuity code supported by a continuity manager and other continuity planners visubcomponent levels throughout the organization or government. as agency management in the Statewide Information Security Man Continuity Facilities Remove The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Remove Term was removed Continuity of Government (COG) Modify Term was removed Continuity of Government (COG) Remove Term was removed Term was removed Term was removed SIRP Add Acronym Computer Security Incident Response Plan, See, Incident Response Plan, See, Upder Incident Response Team, See, Cyber Incident Response Team (CRIT) Add Acronym Add Cyber Threat Actor (CTA) Add Acronym Add Cyber Threat Actor (CTA) Add Acronym Add Cyber Threat Actor (CTA) Actor (CTA) Add Cyber Threat Actor (CTA) Add Cyber Threat Actor (CTA) Acto	rdinators are	FEMA
responsible for oversight of the continuity program. Continuity code supported by a continuity program. Continuity palaners value subcomponent levels throughout the organization or government. as agency management in the Statewide Information Security Man Continuity Facilities Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Modify Ontinuity of Government (COG) Modify Ontinuity of Government (COG) SIRP Add Acronym Computer Security Incident Response Plan, See, Incident Response Plan, See, Upter Incident Response Team, See, Cyber Threat Actor (CTA) Add Acronym Add Acronym Computer Security Incident Response Team, See, Cyber Incident Response Team (CSIRT). And Acronym Add Acronym Add Acronym Add Acronym Add Acronym Computer Security Incident Response Team, See, Cyber Incident Response Team (CSIRT). And And Acronym Add Acrony	rdinators are	
supported by a continuity planners visus subcomponent levels throughout the organization or government. Somitionator Add Somitionator Continuity Facilities Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Continuity of Government (COG) Modify Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Cyber Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Response (COM) Computer Security Incident Response Plan, See, Incident Re		
subcomponent levels throughout the organization or government. as agency management in the Statewide Information Security Man Contingency Planning policy. The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Modify The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Modify Modify Trem was removed		
ontinuity Coordinator Add Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative, or judicial bracesses under the threat or occurrence of any emergency condition that could disrupt such processes and services. Add Accordinated Effort within the executive, legislative, or judicial bracesses under the threat or occurrence of any emergency condition that could disrupt such processes and services. Add Accordinated Effort within the executive, legislative, or judicial bracesses under the threat or occurrence of any emergency or threat. Continuity of government is intended to pres and constitutional authority of elected officials at all levels of gover United States. The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative, or judicial bracesses under the threat or occurrence of any emergency or threat. Continuity of government is intended to pres and constitutional authority of elected officials at all levels of gover United States. The preservation, maintenance, or reconstitution of civil governments, termination of continuity of Government (cos) Remove Term was removed Add Acronym Computer Security Incident Response Plan, See, Cyber Incident Response Plan, See, Incident Response Plan, See, Cyber Incident Response Plan, See, Incident Response Plan, See, Cyber Incident Respo		
Add Contingency Planning policy. Ontinuity Facilities Remove The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Ontinuity of Government (COG) Modify Modif		
Intimity Facilities Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative, or judicial brocesses under the threat or occurrence of any emergency condition that could disrupt such processes and services. Modify Ontinuity of Government eadiness Conditions (COGCON) Remove Term was removed Remove Term was removed Remove Term was removed The preservation, maintenance, or reconstitution of civil government's ability to carry that essential functions continue to be performed before, during, a emergency or threat. Continuity of government is intended to pres and constitutional authority of elected officials at all levels of gover United States. Remove Term was removed Remove Term was removed Add Acronym Computer Security Incident Response Plan, See, Incident Response Plan, See, Cyber Incident Response Team, See, Cyber Incident Response Team, See, Cyber Incident Response Team (CIRT) Add Acronym Computer Security Incident Response Team, See, Cyber Incident Response Team (CIRT) Add Acronym Add Acronym Add Acronym Add Acronym Add Acronym An individual or a group posing a cyber threat. This threat can be diwithin an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous some phosons using the Internet. Threats can come from numerous organization by trusted users or from numerous control to still governments, terrorist groups, disgruntled employees, and intruders. Add Individual or a group posing a cyber threat. This threat can be diwithin an organization by trusted users or from numerous control to still governments, terrorist groups, disgruntled employees, and intruders. Add Acronym Add Acronym Add Acronym Add Acronym Add Acronym Add Acronym An individual or a group posing a cyber threat. This threat can be diwithin an organization by trusted users or from numerous control to still the processes and services. An individual or a group posing a cyb		FEMA
The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative, or judicial bra out the executive, legislative and judicial processes under the threat or occurrence of any emergency or threat. Continuity of government is intended to pres and constitutions continue to be performed before, during, a may emergency condition that could disrupt such processes and services. Term was removed Term was removed Term was removed SIRP Add Acronym Computer Security Incident Response Plan, See, Incident Response Plan, See, Incident Response Team, See, Cyber Incident Response Team, See, Cyber Incident Response Team, See, Cyber Incident Response Team CIRT) Add Add Acronym An individuals usually consisting of Security Analysts organize recommend, and coordinate immediate mitigation actions for conteractication, and recovery resulting from computer security incident Computer Security Incident Response Team (CSIRT). An individual or a group posing a cyber threat. This threat can be divitin an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous sourch hostile governments, terrorist groups, disgrantled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child		FEMA
out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services. Modify Modif		FEIVIA
any emergency condition that could disrupt such processes and services. emergency or threat. Continuity of government is intended to present and constitutional authority of elected officials at all levels of government (COG) Modify Term was removed Term was removed SIRP Add Acronym Computer Security Incident Response Plan, See, Incident Response Plan, See, Incident Response Plan, See, Incident Response Plan See, Cyber Incident Response Pl		
and constitutional authority of elected officials at all levels of gover United States. Modify ontinuity of Government (COGON) Remove Term was removed SIRP Add Acronym Add Acronym TA Add		
Continuity of Government (COG) Modify Continuity of Government (COGCON) Continuity of Government (COGCON) Continuity of Government (COGCON) Continuity of Government (COGCON) Computer Security Incident Response Plan, See, Incident Response Plan, See, Incident Response Plan, See, Incident Response Plan, See, Cyber Incident Response Plan, See, Incident Response Plan,	*	
Term was removed Signer Add Acronym Computer Security Incident Response Plan, See, Incident Response Plan, See, Cyber Incident Response Plan, See, Incident Response Pla	nment across the	
Readiness Conditions (COGCON) Remove Term was removed Add Acronym Computer Security Incident Response Plan, See, Cyber Incident Response Team, See, Cy		FEMA
CSIRP Add Acronym Computer Security Incident Response Plan, See, Incident Response Plan, See, Incident Response CSIRT Add Acronym Computer Security Incident Response Team, See, Cyber Incident Response Team (Cyber Threat Actor (CTA) Add Coordinate immediate mitigation actions for context of computer Security Incident Response Team (CSIRT). An individual or a group posing a cyber threat. This threat can be diswithin an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous sourch hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furtisuch as committing fraud, trafficking in child pornography and intel		
Add Acronym Computer Security Incident Response Team, See, Cyber Incident Response Team, See, Cyber Incident Response Team Cyber Incident Response Team Computer Security Analysts organize recommend, and coordinate immediate mitigation actions for contemporary resulting from computer security incident Response Team CIRT) Add Computer Security Incident Response Team (CSIRT). An individual or a group posing a cyber threat. This threat can be diswithin an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous sourch hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intel		FEMA
Add Acronym Computer Security Incident Response Team, See, Cyber Incident Response Team, See, Cyber Incident Response Team, See, Cyber Incident Response Team CIRT) Add Acronym Crops individuals usually consisting of Security Analysts organize recommend, and coordinate immediate mitigation actions for contend eradication, and recovery resulting from computer security incident CIRT) Add Computer Security Incident Response Team (CIRT) An individual or a group posing a cyber threat. This threat can be diswithin an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furtise such as committing fraud, trafficking in child pornography and intel	Plan	NIST
Add Acronym Cyber Threat Actor Group of individuals usually consisting of Security Analysts organize recommend, and coordinate immediate mitigation actions for cont eradication, and recovery resulting from computer security incident CIRT) Add Computer Security Incident Response Team (CSIRT). An individual or a group posing a cyber threat. This threat can be di within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furtle such as committing fraud, trafficking in child pornography and intel	sponse Team.	NIST
Group of individuals usually consisting of Security Analysts organize recommend, and coordinate immediate mitigation actions for cont eradication, and recovery resulting from computer security incident (CIRT) Add Computer Security Incident Response Team (CSIRT). An individual or a group posing a cyber threat. This threat can be di within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furtle such as committing fraud, trafficking in child pornography and intel		
recommend, and coordinate immediate mitigation actions for cont eradication, and recovery resulting from computer security incident CIRT) Add CIRT) Add An individual or a group posing a cyber threat. This threat can be di within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intel	d to develop	
eradication, and recovery resulting from computer security incident CIRT) Add Computer Security Incident Response Team (CSIRT). An individual or a group posing a cyber threat. This threat can be di within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intel	• •	
CIRT) Add Computer Security Incident Response Team (CSIRT). An individual or a group posing a cyber threat. This threat can be di within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intel		
An individual or a group posing a cyber threat. This threat can be di within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. Add A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intelligence.		NUCT
within an organization by trusted users or from remote locations by persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intell		NIST
persons using the Internet. Threats can come from numerous source hostile governments, terrorist groups, disgruntled employees, and intruders. Add Add Acyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intelligence.		
hostile governments, terrorist groups, disgruntled employees, and intruders. A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intel		
A cyber Threat Actor (CTA) Add A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intel	_	
A cyber threat actor who uses a computer as an instrument to furth such as committing fraud, trafficking in child pornography and intel	nalicious	
such as committing fraud, trafficking in child pornography and intel		NIST, DHS-CISA
such as committing fraud, trafficking in child pornography and intel	ier illegal ends,	
	-	Encyclopedia
ybercriminal Add stealing identities, or violating privacy.		Britannica
AS Add Acronym Emergency Alert System		FEMA
IndEx Add Acronym End of Exercise		FEMA
nd of Exercise (EndEx) Add Actionym Add Actionym The official conclusion of an exercise.		FEMA
		LIVIA
The ground truth is comprised of the detailed elements of a preven		
scenario that must remain consistent during exercise development		
ensure that realism is maintained and objectives may be met in the		
countermove exercise environment. The ground truth includes the	•	
local threat environment, simulated threat group, and individual ad	•	
and relationships. Once composed, the ground truth is used as the	scenario timeline,	
Scenario Events List (MSEL) development and red team operations	scenario timeline, versary profiles	
Ground Truth Add applicable.	scenario timeline, lversary profiles basis for Master	FEMA
Computer hacking (as by infiltration and disruption of a network or	scenario timeline, versary profiles basis for Master planning, if	FEIVIA
Hacktivism Add further the goals of political or social activism.	scenario timeline, lversary profiles basis for Master planning, if	FEIVIA



Term	Action	Description/Notes	Current Definition	New Term/Definition	Source
				HOD is a terminal emulator that provides browser-based or non-browser-based	
Host on Demand (HOD)	Add			client access to IBM mainframe resources.	IBM
				A "Hot Wash" is a post-action review completed within 24 hours of an incident or	
				exercise (or as soon as practical). It is imperative that this review is kept positive in	
				tone; finger-pointing is not constructive and will prevent the honest dialog required	
Hot Wash	Add			The state of the s	FEMA
				The improvement plan identifies specific corrective actions, assigns them to	
				responsible parties, and establishes target dates for their completion. The	
Improvement Plan	Add			improvement plan is developed in conjunction with the After-Action Report.	FEMA
				The documentation of a predetermined set of instructions or procedures to detect,	
				respond to, and limit consequences of a malicious cyber attack against an	
Incident Response Plan	Add			organization's information systems(s).	NIST
				An entity with authorized access that has the potential to harm an information	
				system or enterprise through destruction, disclosure, modification of data, and/or	
nsider Threat	Add			denial of service.	NIST
IRP	Add	Acronym		Incident Response Plan	NIST
MSEL	Add	Acronym		Master Scenario Events List	FEMA
				The MSEL is a chronological timeline of expected actions and scripted events to be	
				injected into exercise play by controllers to generate or prompt player activity. It	
				ensures necessary events happen so that all objectives are met. Larger, more	
				complex exercises may also use a procedural flow, which differs from the MSEL in	
				that it contains only expected player actions or events. The MSEL links simulation to	
Master Scenario Events List				action, enhances exercise experience for players, and reflects an incident or activity	
(MSEL)	Add				FEMA
,			A nation state threat actor is a type of Advanced Persistent Threat (APT). The nation	National cyber warfare programs that pose threats that range from propaganda and	
			state threat actor receives direction and support from an established nation state	low-level nuisance web page defacements to espionage and serious disruption with	
			(government). The line between nation-state cyber activity and cybercrime is often	loss of life and extensive infrastructure disruption	
		Renamed term from "Nation State"	blurred as organized crime groups are afforded a degree of support.	loss of the drid extensive himastrastare disraption	
Nation-State Threat Actor	Modify	and modified definition	and the district of support.		DHS-CISA
Tration State Inicat Actor	ividuity	and modified definition	In the agency's opinion, the loss of an application will have little or no impact to	See , Application Criticality or Process Criticality.	D113 C13/1
			Statewide and/or agency core functions, processes and activities or the core functions,		
Non-Critical	Modify		processes and activities associated with a program within the agency.		FEMA
THOR CITERCAL	ivicumy		processes and detivities associated with a program within the agency.	The actions taken to plan, organize, equip, train, and exercise to build and sustain	1 21417 (
				the capabilities necessary to prevent, protect against, mitigate the effects of,	
				respond to, and recover from those threats that pose the greatest risk to the	
Preparedness	Add			· · ·	FEMA
r repareuriess	Auu		An account of an information system that has more authority and accoss than a	An account of an information system that has elevated or special access or more	LIVIA
			An account of an information system that has more authority and access than a		
			normal user account. Examples of privileged accounts include those that have root	authority than a normal user account. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with	
Privilaged Assount	Modify		access, system administrator access, and accounts associated with database		NC DIT
Privileged Account	ividuity		ownership and router access.		INC DIT
				Process Criticality – Process criticality has the following categories.	
				Chatanida Cikiral Basadan tha areas da anchair this ann an dias this and	
				• Statewide Critical – Based on the agency's analysis, this process has a direct impact	
				to statewide essential functions, processes, activities or population.	
				• Agency Critical – Based on the agency's analysis, this process has a direct impact to	
				the agency's essential functions, processes and/or activities.	
				• Program Critical – Based on the agency's analysis, this process has a direct impact	
				to the essential functions, processes and/or activities associated with a program	
				within the agency.	
				• Non-Critical – Based on the agency's analysis, this process has no direct impact to a	
				state, agency, or program's essential functions, processes and activities within the	
Process Criticality	Add				FEMA
				See , Application Criticality.	
			application will have a direct impact to the core functions, processes and/or activities		
Program Critical	Modify		associated with a program within this agency.		FEMA
	,				



Term	Action	Description/Notes	Current Definition	New Term/Definition	Source
			All documents, papers, letters, maps, books, photographs, films, sound recordings,	As defined by N.C.G.S 132-1, all documents, papers, letters, maps, books,	
			magnetic or other tapes, electronic data-processing records, artifacts, or other	photographs, films, sound recordings, magnetic or other tapes, electronic data-	
			documentary material, regardless of physical form or characteristics, made or received	processing records, artifacts, or other documentary material, regardless of physical	
			pursuant to law or ordinance in connection with the transaction of public business by	form or characteristics, made or received pursuant to law or ordinance in connection	
			any agency of North Carolina government or its subdivisions.	with the transaction of public business by any agency of North Carolina government	
Public Records	Modify			or its subdivisions.	NC DIT
RCA	Add	Acronym		Root-Cause Analysis	FEMA
			Formal statement by a department that it is soliciting enterprises to bid on a contract	Formal statement by an organization that it is soliciting vendors to bid on a contract	
Request for Proposal (RFP)	Modify		for a program, system or service.	for a program, system or service.	NC DIT
				When evaluating exercises, root-cause analysis involves not merely identifying what	
				issues emerged, but rather discovering the root causes of those issues. Root-cause	
				analysis enables exercise stakeholders to target how best to address areas for	
Root-Cause Analysis (RCA)	Add			improvement and close capability gaps.	FEMA
			The use of more than one individual to handle a particular (generally important)	The use of more than one individual to handle a particular (generally important)	
			activity.	activity to distribute the associated privilege of authority among multiple individuals	
				or entities. The goal is to eliminate the possibility of a single user or entity from	
Separation of Duties	Modify			carrying out and concealing a prohibited action.	OWASP
SISM	Add	Acronym		Statewide Information Security Manual	
SME	Add	Acronym		Subject Matter Expert	FEMA
StartEx	Add	Acronym		Start of Exercise	FEMA
Start of Exercise (StartEx)	Add			The official beginning of an exercise.	FEMA
				SMEs have functional knowledge and expertise in a specific area or in performing a	
				specialized job, task, or skill. As part of an exercise planning team, they help make	
				the scenario realistic and plausible and ensure agencies and/or the state has the	
				appropriate capabilities to respond. SMEs are ideal for the positions of controllers	
Subject-Matter Expert (SME)	Add				FEMA
				A TTX is typically held in an informal setting intended to generate discussion of	
				various issues regarding a hypothetical, simulated emergency. TTXs can be used to	
				enhance general awareness, validate plans and procedures, rehearse concepts,	
				and/or assess the types of systems needed to guide the prevention of, protection	
				from, mitigation of, response to, and recovery from a defined incident. Generally,	
				TTXs are aimed at facilitating conceptual understanding, identifying strengths and	
				areas for improvement, and/or achieving changes in attitudes.	
Tabletop Exercise (TTX)	Add				FEMA
TLD	Add	Acronym			IETF, RFC 1591
TT&E	Add	Acronym		1	FEMA
TTX	Add	Acronym		, - 0,	FEMA
		,	Measures to ensure that an organization's Continuity plan is capable of supporting the	·	
			7		
Tests, Training, and Exercises			of a Continuity event. TT&E activities are designed to familiarize, impart skills and	supporting the continued execution of the organization's essential functions	
(TT&E)	Modify		ensure viability of Continuity plans.		FEMA
			An intentional or accidental action, activity or event that can adversely impact agency	Any circumstance or event with the potential to adversely impact organizational	
			information assets, as well as the sources, such as the individuals, groups, or	operations (including mission, functions, image, or reputation), organizational assets,	
			organizations, of these events and activities.	individuals, other organizations, or the Nation through an information system via	
				unauthorized access, destruction, disclosure, modification of information, and/or	
Threat	Modify				NIST
24.5				In the Domain Name System (DNS) naming of computers there is a hierarchy of	
				names. The root of system is unnamed. There are a set of what are called "top-level	
				domain names" (TLDs). These are the generic TLDs (.EDU, .COM, .NET, .ORG, .GOV,	
				.MIL, and .INT), and the two letter country codes (e.gUS, .CA, .EU, etc.) from ISO-	
Ton Loyal Damain	ı			, , , , , , , , , , , , , , , , , , , ,	LETE DEC 4504
Top-Level Domain	Add			3166.	IETF, RFC 1591